

AU/ACSC/2015

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

**LESSONS FROM THE FRONT:  
A CASE STUDY OF RUSSIAN CYBER WARFARE**

By

Max Gordon, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Dennis Duffin

Maxwell Air Force Base, Alabama

December 2015

DISTRIBUTION A. Approved for public release: distribution unlimited.

## **Disclaimer**

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.



## TABLE OF CONTENTS

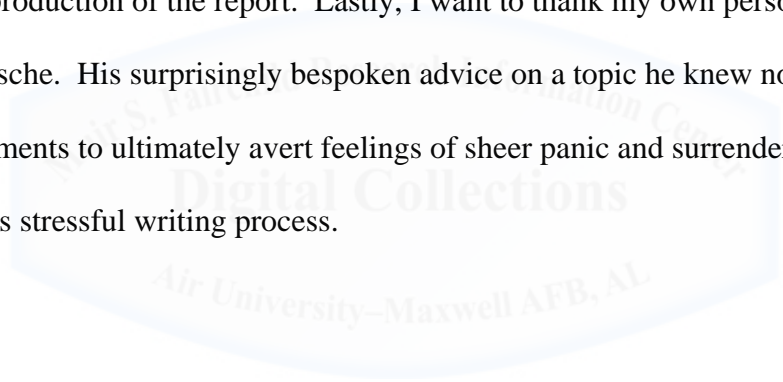
	<i>Page</i>
DISCLAIMER .....	ii
ACKNOWLEDGEMENTS .....	v
ABSTRACT.....	vi
 CHAPTER ONE – LEARNING FROM THE PAST .....	 1
Research Question .....	1
CHAPTER TWO: SETTING THE STAGE .....	3
Research Methodology .....	3
Key Terms and Concepts .....	4
CHAPTER THREE – CASE STUDIES .....	7
Case Study Methodology .....	7
Case Study One: Russia V. Estonia .....	7
Conflict Catalyst .....	7
National Cyber-Conflict .....	8
Result .....	10
Case Study Two: Russia v. Georgia .....	11
Conflict Development.....	11
The First Cyber War .....	12
Result .....	14
CHAPTER FOUR – RESEARCH CONSIDERATIONS .....	16
Consideration I: Small Sample Size .....	16
Consideration II: Asymmetric v. Symmetric .....	16
Consideration III: Hacktivists .....	17
Consideration IV: Observer Effect .....	17
CHAPTER FIVE – CYBER-WARFARE ANALYSIS.....	19
The Silent Killer.....	19
The Indications and Warnings of Integrated Cyber-Warfare.....	21
Tools and Tactics .....	22
CHAPTER SIX – CONCLUSIONS AND RECOMMENDATIONS.....	27
Conclusion I: Cyber-Attacks Inside and Outside of War.....	27
Recommendation I: Protocol for Proportional Cyber-Response .....	28
Conclusion II: Integrated Domains of Warfare.....	29

Recommendation II: Cyber-ISR Assessment Teams .....	30
Conclusion III: Taking Advantage of Tech-Dependence .....	31
Recommendation III: Evolving DDoS Mitigation and Cyber-ATSO Training .....	32
Recommendations for Future Research .....	34
Report Summary .....	35
ENDNOTES .....	37
BIBLIOGRAPHY .....	40



## ACKNOWLEDGEMENTS

In the long quest to complete this research, I would like to thank the following saints. First and foremost, my wonderful wife deserves the lion's share of my appreciation as this report would not exist without her constant patience and loving support, despite me sneaking off for hours to perform caffeine-fueled research while she was left corralling two angst-filled adolescents. I want to thank my fellow students as well as my report advisor, the patient and alliterative Dr. Dennis Duffin for his constant reminders and carefully placed corrections. He managed to strike the perfect balance of providing guidance while not inserting himself too much into the overall production of the report. Lastly, I want to thank my own personal English teacher, Ross Tasche. His surprisingly bespoken advice on a topic he knew nothing about came at opportune moments to ultimately avert feelings of sheer panic and surrender on the part of the author during this stressful writing process.



## ABSTRACT

“Lessons From The Front: A Case Study Of Russian Cyber Warfare” looks to capitalize on the lessons learned from the alleged Russian cyber-offensive on Estonian networks in 2007 and the conflict that erupted in South Ossetia in 2008 following prolonged destabilizing efforts on the part of Russia. The goal of this research is to improve the United States Air Force (USAF) outlook in future conflicts by extrapolating the likely cyber-tactics to be utilized by a technically symmetric adversary, and how the USAF can use this knowledge to better protect itself. This research question is answered through the careful analysis and comparison of two disparate conflicts related by their collision with Russian cyber-warfare. Following case study discussion of Estonia and Georgia, the two cases are analyzed and discussed to study the Russian tactics that were used effectively during these conflicts. Based on this research and analysis, the following conclusions were made.

A sophisticated cyber-offensive on the USAF will most likely involve the following:

- Cyber-attacks on target systems will not be limited to states of declared war
- The cyber domain will be integrated with Land, Sea, Air, and Space campaigns
- Adversary will capitalize on the USAFs tech-dependence by degrading C2 picture

In light of these conclusions, the report recommends the USAF does the following:

- Pursues an internationally accepted protocol for proportional cyber-responses
- Utilizes education programs to develop Airmen that can exploit the inherent weaknesses involved in an integrated cyber-offensive
- Maintains responsive DDoS mitigation capabilities and exercises its Airmen in how to operate in a degraded technological state.

## **CHAPTER ONE – LEARNING FROM THE PAST**

The United States Air Force (USAF) has created a relatively new Operations Center (OC) in the 624<sup>th</sup> to exercise full-spectrum cyberspace operations throughout the Air Force Information Network (AFIN). One of its many functions is to defend the AFIN from cyber-attacks, to include the fairly prolific Distributed Denial of Service (DDoS) attacks. This has never been tested in a wartime situation, yet this does not preclude the USAF from utilizing the experience of others in order to prepare for such an occurrence. Between 2007 and 2008, Russia was involved in cyber-conflicts with both Estonia and Georgia. In both cases Russia employed effective cyber-tactics, to include DDoS attacks as well as several other cyber-measures, against these smaller states to debilitate their capabilities and communications during both peacetime and wartime conflict.<sup>1,2</sup>

### **Research Question**

Should a highly capable state with technically advanced abilities like Russia or China choose to employ cyber to debilitate the US military's offensive and defensive capabilities, the USAF needs to be capable of "surviving" or mitigating the attack such that it can continue to operate. Mitigating a cyber-attack can mean many different things, so "mitigating" in this case means either stopping the attack before it affects its target, or that after initially weathering the attack, the USAF is able to quickly stand the network back up and respond to the threat at such a level that the enemy is unable or unwilling to continue the attack. The purpose of this research is to answer the question: *"Based on the recent Russian conflicts with Estonia and Georgia, what kinds of cyber-tactics can the USAF expect a technically symmetric adversary to use in possible future cyber-offensives?"* Once a baseline for major state tactics and capabilities has been

established through this report, it can be used by future scholars from the various services and backgrounds as a springboard for further analysis on conflicts as they are sure to arise. Ideally, this in turn will improve the international community of knowledge on the subject of cyber-warfare.

Outside of the kinetic realm, the extent of permanent damage one can do to an enemy network is very limited in scope. Even if the adversary is able to launch a significant cyber campaign, the effect will usually be a temporary one. Where an adversary can gain the advantage then, is by using a DDoS type attack in concert with or prior to a kinetic attack in hopes of either “blinding” the enemy or at least slowing them down. In a peacetime state, the USAF defends the AFIN against thousands of smaller versions of these cyber-attacks each year.<sup>3</sup> While the potency of cyber-attacks has grown exponentially over the years, the authors of these attacks have largely been non-state actors and small groups of individuals. Consequently, mitigation of these types of cyber-attacks has been built around defending against the capabilities of asymmetric attackers while ignoring the cyber capabilities of symmetric adversaries.

The significance of a major power like Russia or China utilizing cyber-attacks like DDoS is not the damage it would do the AFIN, but what that attack would portend. Even a temporary takedown of the AFIN would significantly improve the adversary’s chances to gain the upper-hand in a physical attack. Due to the relative infancy of this type of warfare, there is a dearth of information available for the warfighter to draw upon in order to prepare for it. By analyzing the cyber –warfare that occurred during the Russia v. Estonia and Russia v. Georgia conflicts, the US Air Force can get a better idea of how a technically symmetric adversary might prosecute a cyber-attack during or in the run-up to a physical conflict.



## **CHAPTER TWO: SETTING THE STAGE**

### **Research Methodology**

Since the advent of effective cyber weapons in the 21<sup>st</sup> century, there is a very finite number of state conflicts where cyber was utilized as a weapon. This report is focused on a case-study of two fairly small cyber-conflicts, significant due to their recency and the alleged use of cyber by a major world power like Russia. While DDoS is one of multiple methods of cyber-attack allegedly utilized by Russia, DDoS appears to be *de rigueur* for Russian hackers and therefore garners specific discussion during the analysis. This research attempts to ascertain Russian tactics and capabilities as a major state-actor in the world of cyber warfare.

There is no panacea for solving the unknowns of an adversary's cyber-warfare tactics. Researching state-led cyber-attacks is fairly new terrain with limited resources to extract information from. More fidelity of knowledge in enemy cyber-warfare tactics and major state DDoS capabilities is needed in order to assess how well the USAF can protect its networks in the face of a major world power. Following the background and initial analysis of the two conflicts, a discussion on the limitations of these case studies as well as in-depth analysis will be conducted. The conclusions in this report on Russian cyber-tactics and capabilities will assist in speaking to the future of the USAF's cyber-mitigation capabilities and address recommendations for what can be done to modify or improve current wartime tactics and best practices inside and outside the cyber-domain.

Its importance has long been underdeveloped by the armed forces, and the research on cyber-warfare is still in its infancy. Every branch of the US military and possibly some government agencies will face this type of threat in a time of war, so improving the warfighter's

knowledge on this subject will make the Whole of Government (WoG) stronger. It is hoped that once this evaluation is complete, the warfighter will have a better understanding of where the USAF capabilities stand in relation to the threat, and more importantly, where they should be.

## **Key Terms and Concepts**

This report covers various technical concepts, and as such it is imperative that these concepts and the terms used alongside are understood by the reader. The first of these concepts is the Distributed Denial of Service attack, or DDoS. The DDoS method of cyber-attack is not new; in fact, it has been around for almost as long as the internet itself.<sup>4</sup> It is important to understand this type of cyber-attack since it is one of the most powerful tools that hackers, state-sponsored or otherwise, can use to attack the AFIN. Every server has a certain amount of bandwidth that it can handle, and if asked to go beyond that it will shut down. Simply put, a DDoS attack overloads the server it is attacking, and the result is that the targeted server crashes, effectively denying service to its users. This is precisely why this research is important; the implications of an enemy state being able to take down the AFIN are far reaching. The USAF is a highly technical service that is heavily dependent on being able to access myriad applications that enable the command and control (C2) of air, space, and missile assets. Running a 21<sup>st</sup> century military force without the use of those computers and applications would severely degrade the USAF's capabilities.

The fact that DDoS has stood the test of time speaks to how effective it is; many systems, despite their cyber security, can still be affected by this method of attack. DDoS has been used to take down "hard" targets like CIA.gov, and has even been used to take down the entire network infrastructure of small countries as will be shown in the two case studies to follow.<sup>5</sup>

Most of these attacks are fairly inexpensive to carry out and the manning required can be quite small. A stark example of this is the server takedown of the Central Intelligence Agency (CIA). Two teenagers from the United Kingdom (UK) were the culprits.<sup>6</sup> One of the best ways to defend against a DDoS attack is to escape the notice of attackers, and so far the AFIN has escaped the notice of most prominent DDoS hacking groups, but this will not be a valid tactic if the US military is the focus of the attack. The USAF has gotten used to defending against the constant threat of hacker infiltration into the AFIN, and while the USAF has seen DDoS attacks on a smaller scale, it has not had to deal with a concentrated DDoS attack from a major player like Russia.<sup>7</sup>

Another important term to understand is the Air Force Information Network. “The AFIN is the globally interconnected, end-to-end set of AF unique information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel...”<sup>8</sup> In layman’s terms, if an Airman is working on a government computer, that Airman is working within the AFIN. For an adversary to attack USAF computer-based systems and take them offline, it would need to be able to penetrate the AFIN or disable it.

The most challenging aspect of answering this question of whether or not the USAF can utilize these case studies to learn from past experiences, is in determining what the enemy is capable of bringing to bear against the USAF. Short of asking a country like China to just show their hand, so to speak, it is difficult to procure an iron-clad answer to this. Fortunately, Russia has possibly tipped their hand by allowing others to witness their cyber-tactics. However, even when specific information on these tactics is accessible, it is not an exact science, and DDoS capabilities are constantly evolving to where the conclusions of this report can become obsolete

fairly quickly if not colored with possible limitations.<sup>9</sup> These limitations are discussed in-depth later in the report.

Fortunately (or unfortunately), DDoS attacks are occurring all the time, and while these are not necessarily carried out by major world powers, an educated estimate on the DDoS capabilities of these major powers can be extrapolated by analyzing the existing metrics on DDoS attacks that happen daily throughout the world. Additionally, this information could be compared against cases where a country like Russia or China was involved, in order to get an idea of what one would expect of a future DDoS attack from one of these countries vs. relatively low-level hackers. However, until a major war occurs involving the use of cyber, it can be assumed that major powers will limit the full capabilities available to them in the cyber-realm in order to protect those capabilities.



## **CHAPTER THREE – CASE STUDIES**

### **Case Study Methodology**

Now that a basic overview of the report's organization has been reviewed, this report will now move into the two conflicts discussed. Each case study begins with a succinct background on the conflict in question, a look at the cyber-tactics utilized, the effects to the target country, and the response or fallout that occurred as a result. Following the Case Studies, this report moves into a discussion on the application of the tactics utilized in these case-studies and their implications for the USAF and the military writ-large.

### **Case Study One: Russia v. Estonia**

#### **Conflict Catalyst**

A critical point to understand in the origin of this conflict is that Russia continues to feel a sense of ownership over its former Soviet states. Estonia, previously a ward of the now dismantled Soviet Union, is comprised like many others around it, that is to say the population is a mixture of ethnic Estonians and Russians alike due to the active "Russification" of the Eastern Bloc during the Cold War.<sup>10</sup> As has been recently seen in Ukraine, Russia sees these Russian Diasporas as still part of its domain and is therefore very sensitive to actions that might threaten the status-quo. There were mounting political tensions between Estonia and Russia over the bronze statue of a Soviet soldier that ostensibly commemorated the Soviet's role in fighting the Nazi offensive. Estonia wished to move the statue because it had eventually become a reminder of five decades of Soviet occupation.<sup>11</sup>

On April 27, 2007, the statue was finally moved from central Tallinn to a less prominent

location within the city.<sup>12</sup> Adding to the tensions of the situation was the fact that Red Army soldiers buried beneath the statue were also exhumed and moved with the statue. Upon hearing of the removal, that same day President Putin publicly denounced the removal and communicated to Estonia that their actions would have serious consequences.<sup>13</sup> A coordinated offensive of cyber-attacks began on the evening of the removal.

### **National Cyber-Conflict**

This was the first known instance of an entire country being attacked via a massive cyber-offensive. However, calling this a war might be a bit of a misnomer in that the term “war” implies that both sides were fighting. The main thrust of this very one-sided attack began the night of the 27<sup>th</sup> and was perpetrated through the use of botnets, a common form of DDoS created by linking multiple devices together in order to multiply the effects of an attack bent on overloading the targeted system.<sup>14</sup> Government and communications infrastructure appeared to be the focus of the initial attacks, as well as one of Estonia’s popular digital news outlets, Postimees Online.<sup>15</sup> Over the next few days the force of the attacks grew, as well as the list of targets.

One might think Estonia would not be too adversely affected by cyber-attacks, but for a country that has been described as “The Most Wired in Europe,” this was a very effective way to cripple a state that has invested heavily in hi-tech infrastructure.<sup>16</sup> Estonia depends on the Internet for myriad critical functions anywhere from providing banking services to its citizens, to control of the power grid.<sup>17</sup> In a country where online banking transactions near the 100% mark, the population as well as the economy was feeling the effects of these cyber-salvos.<sup>18</sup> Government services were taken down and email servers were dismantled during the attacks.

This was an especially tough blow to an Estonian government described as “paperless” by Mihkel Tammet, head of Information Technology (IT) security at Estonia’s Defense Ministry.<sup>19</sup>

These attacks were all the more impressive in that this was not a case of Estonia being caught unaware. Many IT experts in the country had done an impressive amount of preparation in combating possible threats to web services, due in part to the country’s need for sophisticated security in the face of an early adoption of web-based voting in Estonia. Schmidt points out that “...a task force consisting of security experts from ISPs, election authorities, police, intelligence services, and others was formed to prepare for potential attacks on the elections.”<sup>20</sup> This same task force was reformed in preparation for possible attacks during the elections in April, and was kept on alert after intelligence chatter and information from the Ministry of Defense was warning of possible DDoS attacks on the government.<sup>21</sup>

Unfortunately, Estonia’s defensive options were very limited in the face of the size and sophistication of these attacks. A typical DDoS botnet will be employed by low-level hackers, nicknamed “script-kiddies” with the implication that they are inexperienced kids hacking with copied, pre-fabricated scripts or rented botnets created by more capable hackers. This did not seem to be the case with many of the incoming attacks. One IT expert in Estonia related how he would defeat an incoming DDoS attack by filtering out that botnet’s particular brand of attack, only to see the same one get past the defenses after being modified to bypass the newly placed filter, indicating an active, persistent, and sophisticated hacker was on the other end of that line of attack.<sup>22</sup> These coordinated attacks continued for weeks, culminating in attacks so large that Estonia was forced to do what many of its smaller agencies and services had already done – admit defeat and shut off all internet traffic coming from outside the country, which also meant that Estonia would not be able to communicate to the outside world about the continued assault

on their telecommunications infrastructure.

## **Result**

Russia denied any involvement in these attacks, and as is the case with most cyber-attacks, it is extremely difficult to prove otherwise. Estonian IT experts had tracked the source of many of these attacks to Russia, even going so far as to find one that came from a computer within the Kremlin.<sup>23</sup> This is far from being a smoking gun as botnets are compiled through the collection of multiple, unsuspecting computers; however, many scholars who subsequently studied the nature of the attacks came to the same conclusion as Estonia on the culprits involved.<sup>24</sup> Regardless of whether or not Russia's denial would stand up in an international court, for the purposes of this report, this conflict provides the USAF with a stellar example of what kind of fallout can occur within a defensive command and control structure if a large-scale, coordinated cyber-offensive is used.

An important note about this cyber-offensive is that there were almost zero lasting effects to Estonia following the weeks of attacks because of the inherent nature of cyber-attacks. This is not to imply that damage cannot be done, as will be noted in the discussion following these case studies, but as far as Russia v. Estonia is concerned, there was very limited permanent damage. While a comprehensive damage assessment was not done simply due to the lack of monitoring and recording of attack actions, a government server had to be rebuilt, and it is estimated that multiple millions of dollars were lost by banking institutions, government services, and Estonian newspapers; the infrastructure for the most part remained intact.<sup>25</sup> One scholar concluded that Estonia was able use the experience and even the political fallout to their advantage by bolstering relationships and commitments from NATO members and improving their IT security by



learning from the situation. This attitude of learning from the past is the very focus of this report and should be kept in mind as the report moves into the second case-study.

## **Case Study Two: Russia v. Georgia**

### **Conflict Development**

Like Estonia, Georgia has a checkered history with Russia. A former part of the United Soviet Socialist Republic (USSR), Georgia became independent upon the dissolution of the Soviet Union in 1991.<sup>26</sup> The year prior to the fall of the Soviet Union, an area in northern Georgia called South Ossetia attempted to separate from Georgia and declare its independence, an action which led to the South Ossetian-Georgian Conflict.<sup>27</sup> The result of that war was a cease-fire between Georgia, Russia, and Pro-Russian fighters in South Ossetia.

From the declaration of Ossetian independence in 1990 until the 2008 Russo-Georgian War, Russia effectively maintained its hold in the area forcibly by keeping a military presence at the ready on the border of Georgia.<sup>28</sup> Economically, it maintained involvement in South Ossetia by providing monetary assistance to the populace and allowing South Ossetians to register as citizens of the Russian Federation.<sup>29</sup>

Pertinent in the discussion to follow is how the conflict finally erupted into what is now known as the Russo-Georgian War. Tensions had slowly been building between Russia and Georgia due in part to Russian exercises overtly designed to prepare Russian troops for a Georgian offensive into South Ossetia in order to simulate the recapture of definitive control of the region.<sup>30</sup> Alternatively, the building tension was not eased by the aggressively destabilizing policies of Georgian leadership vis-à-vis the South Ossetian Region.<sup>31</sup> All of this led to the eventual eruption of conflict on August 7, 2008. Georgian troops, purportedly in response to separatist aggression in the region, moved into South Ossetia to reestablish control and were

subsequently met by Russian troops.<sup>32</sup>

## **The First Cyber-War**

While the Russia v. Estonia conflict was significant due to it being the first known case of a country coming under attack via cyber, Russia v. Georgia is even more significant in that it is the first known use of cyber in tandem with a conflict in the physical domain.<sup>33</sup> Interestingly enough, one could argue that the war had started prior to Georgian troops coming into contact with their adversary. Three weeks prior to conflict in the physical realm, a cyber-offensive from Russian hackers had already begun. These attacks were coordinated and for the most part came in the form of DDoS, as was seen in Estonia. Though the physical war began in August, one of Arbor Networks' security researchers was witnessing DDoS attacks on Georgian government websites as early as 20 July.<sup>34</sup>

One could look at these early attacks as probes for weakness or early exercises for government hackers, however it is just as likely that these attacks prior to physical conflict were simply rogue "hacktivists" from within Russia. In a manner that appeared perfectly synchronized, Russian troops marched into South Ossetia to protect their interests in the area and keep Georgia from asserting power over the region militarily while more cyber-attacks flooded into Georgian websites. The DDoS attacks were effective in shutting targeted websites down and disrupting communication from Georgia to the outside world. As was the case with the website for the Georgian parliament, some websites were not shut down but instead defaced with Russian propaganda.<sup>35</sup>

The Russian hackers, government sanctioned or no, seemed to be well coordinated and tactically sound in their actions. Just as an airstrike into an enemy country would first target the

enemy's defensive capabilities such as Air Defense Artillery (ADA), the attacks in August began by targeting frequented Georgian hacker forums.<sup>36</sup> By effectively neutralizing the enemy before they could counter the attacks, Russian hackers ensured their dominance against the already overwhelmed Georgian web infrastructure. Another sophisticated tactic of Russian hacking capability was the timing and location of these cyber-attacks.

While Russia maintains that only Russian civilians were involved in nefarious hacking activities, the hackers seemed to know where Russian attacks would occur before they happened, and instead of attacking websites at random, specific and militarily significant sites were targeted. For example, a report from the US Cyber Consequences Unit (USCCU) on the attacks noted that a Georgian website shut down by hackers was used for renting diesel-powered generators; a highly unlikely target for Russian "hacktivists" or bored script-kiddies; much more likely a perpetrator looking to "...reinforce the effects of physical strikes on the Georgian power-grid."<sup>37</sup>

Not only does it appear that the hackers were taking their cues from the Russian military, the military seemed to also be paying attention to what targets had been taken offline by the hackers. Russian target selection in Georgia appeared to be in coordination with attacks in the cyber-domain; command and control centers and news media outlets, physical targets that would normally be high on the list for Russia to hit in order to control communication from within Georgia, seemed to be spared since they had already been neutralized via cyber.<sup>38</sup> Further, the hacker's involvement with the military was also betrayed by the targets they did *not* hit. The USCCU noted that many critical Georgian infrastructures were accessible to hackers during the attacks, and that had they wanted to do lasting damage to some of these systems it would have been well within the capabilities displayed during the war.<sup>39</sup> Again, instead of the frenetic,

destructive nature that is usually noted with disorganized hacker communities, they were instead demonstrating restraint and foresight in their choice of targets.

## **Result**

While some of these cyber-attacks may sound similar and even more egregious than what occurred in Estonia, the majority of the Georgian population was unaffected by these cyber-attacks. Militarily the cyber-attacks seemed to assist in the overall strategic goal of the Russian military, but Georgian civilian life was not crippled by the cyber-attacks during the war. The difference-maker here was that Georgia was nowhere near as cyber-dependent as was Estonia. Around the same time as this conflict Estonia had approximately 57 out of 100 citizens on the web; Georgia had merely 7.<sup>40</sup> In this way the general populace of Georgia felt nowhere near the same effects of these cyber-attacks as did Estonian citizens.

Again, Russia denied any involvement in these cyber-attacks on Georgia. While this is unsurprising, it is somewhat telling that Russia still denies involvement in the cyber-domain while being very obviously involved in an open conflict with Georgia. Some of the cyber-attacks that occurred, to include the defacement of the Parliament websites, were prepared years in advance. That is not the planning of a fair-weather hacker getting in on the fun of a Russian conflict.<sup>41</sup> The question then becomes, what is more likely: Russia utilizing a cheap, effective means of attack that it is perfectly capable of using in an open war against Georgia, or that a large band of disorganized Russian amateur hackers planned years in advance to attack Georgia via cyber in a way that coincided perfectly with Russian operational and tactical objectives? Russia undoubtedly wishes to keep its capabilities in the cyber-domain “off the radar,” but it is at best naïve for Russia to continue to deny any involvement in said attacks.

It should also be noted that while Georgia is much more behind technologically speaking than Estonia was, it was more accurate to call this cyber-warfare because Georgian hackers returned fire when able, where Estonia simply cut off outside access to its websites, effectively becoming an *intranet*. Currently, South Ossetia remains under contention; occupied by the Russian military but generally still recognized by the international community as part of Georgia.<sup>42</sup>



## **CHAPTER FOUR – RESEARCH CONSIDERATIONS**

As with any research, there can be limitations to the material under analysis; therefore it is incumbent upon the researcher to ensure the reader is aware of all aspects of an argument to encourage the consideration of alternative possibilities and conclusions. As a precursor to the comparison and analysis of these case studies and the tactics observed, the following section will cover four research considerations.

### **Consideration I: Small Sample Size**

The objective of this report is to assist the USAF in preparing itself for an eventual conflict with a symmetric adversary. Real-world examples from the past are used to do this. However, since cyber-warfare is a relatively new frontier, real-world examples are few and far between. Therefore it needs to be stressed that the cyber-tactics employed by Russia have not been witnessed ad nauseum; that is to say, this research can only make conclusions based on what has been seen, and there is likely much that still needs to be done in this area of research that can only be done once more conflicts have taken place.

### **Consideration II: Asymmetric v. Symmetric**

The thesis of this report uses the word “symmetric” to describe a country that can match the US in terms of capability in the cyber domain. While the case studies of Estonia and Georgia cover Russia, very much a possible symmetric adversary to the US, in these cases Russia itself is fighting an enemy that is fairly asymmetric. The limitation here is that while an appropriate state

is being looked at, the full extent of Russian capability may not be observed because of who it is fighting.

### **Consideration III: Hacktivists?**

The evidence of Russian government involvement in the cyber-attacks on Estonia is fairly persuasive, and even more so with Georgia. However, because of the difficulty in attributing cyber-attacks and Russia's repeated denials, it must be pointed out that there still exists the possibility that Russia has not been involved at all in these cyber-attacks. For example, Russia argued that it was likely that ethnic Russian's from inside Estonia were to blame for the DDoS attacks on Estonian websites.<sup>43</sup> This appears to only further implicate Russia based on the fact that once Estonia cut-off international internet traffic, the DDoS attacks ceased completely.<sup>44</sup> Regardless, Russia's denials must be noted and considered when utilizing this report and its conclusions in a discussion of large-nation cyber capabilities.

### **Consideration IV: Observer Effect**

Russia has demonstrated a pattern of utilizing cyber-warfare in engagements with an adversary. However, a conservative strategist needs to consider all possibilities when defending against a possible attack. The Observer Effect holds that observing a process can change it. Just by virtue of Russia being aware that their cyber-tactics are being observed on a world stage means that they may change things in future conflicts. With that in mind, while one may come to the conclusion that Russia will continue utilizing cyber-tactics in the same manner, the reader needs to color this conclusion with the fact that Russia is aware that it has "shown its cards," so to speak.

In a future conflict, Russia could easily change tactics to keep the adversary off-guard. For example, in the Russia v. Georgia conflict Russia is observed attacking preemptively with cyber.<sup>45</sup> This example gives the reader one possible tactic, not *the* tactic. Additionally, Russia is just one symmetric adversary of many. Using the example of Russian cyber-tactics to inform on possible activities and tactics of Chinese government hackers could certainly be useful, but must be seasoned with the realization that these are case-studies, and as such do not cover every avenue of possibility when it comes to the capabilities of other symmetric adversaries.





## **CHAPTER FIVE – CYBER-WARFARE ANALYSIS**

Moving now into further analysis of Russian cyber-tactics utilized during the aforementioned conflicts, the following section will cover three overarching tactics, or enemy behaviors that were used effectively by Russian hackers to accomplish political and military objectives. For the aims of this report, Russia v. Georgia is more significant in that it provides for much more concrete examples of cyber-tactics and how they can be used in tandem with physical conflict. However, analyzing and comparing the two lends credence to the conclusions of this report both by establishing a pattern in Russia's prosecution of cyber-tactics, and more importantly, by including Estonia this report is afforded a look at the effects of cyber-attacks on a technically dependent society. While the physical domains were not integrated into that conflict, it may provide context for those who view the cyber domain as a weapon with no kinetic effects.

### **I. The Silent Killer**

As in the case of a clearly guilty criminal getting away with murder due to a technicality, it would be a "fool me twice" type situation if the affected community did not take measures to protect themselves from that individual's future crimes. However, due to the nature of cyber-conflict it can be very difficult to identify the perpetrator of the cyber-attack. Instead of a victimless crime, there is instead a clear victim but the crime is nowhere to be seen. This is pertinent to the discussion because while there is currently no way to effectively prosecute a possible perpetrator like Russia because of the ephemeral nature of cyber, by looking at the case studies of Russia v. Estonia and Russia v. Georgia, it is possible to at least identify a pattern to

the actions of countries prosecuting cyber-offensives. In this way the USAF can determine how the AFIN might be affected by these types of cyber-tactics and how to better protect the network should conflict arise between the US and a technically proficient aggressor.

This section highlights something that this report will dub “cyber-apathy”, or the international community’s acceptance of cyber-attacks as a matter of course. In comparing the two case studies, it is easier to recognize this response in the Estonia case since there was not a physical war to distract from it, i.e. in the case of Georgia it makes no sense to cry foul over cyber-attacks when Russian tanks are rolling across the border. At the heart of this apathy is the question of efficacy. As Rehman puts it, “There is, however, always the issue of how to identify whether a cyberattack is a weapon of mass destruction or simply a weapon of mass distraction and inconvenience.”<sup>46</sup> What he is discussing is how the general populace does not know how to classify cyber-attacks. Further, the world has yet to witness truly damaging cyber-attacks. For the most part, cyber-attacks in the news have tended to be more transitory in nature.

As was discussed earlier, cyber-warfare is so new that the international community has not witnessed the true potential of cyber-attacks. These attacks, while not necessarily kinetic, can have secondary and tertiary effects that are truly devastating. For example, if Russia so desired it could have taught Estonia a much more painful lesson by targeting Estonian infrastructure. Technologically advanced societies have a multitude of what is known as a Cyber Physical System (CPS), typically referring to the integration of physical systems and infrastructures with computer systems.<sup>47</sup> These types of attacks utilized against power-grids, water treatment facilities, or gas/oil distribution facilities could quickly become deadly. Due to the lack of real-world examples and actual body-counts, the international community instead labels attacks on CPS’ as alarmist and unrealistic.<sup>48</sup> It is apparent that Russia counted on this

apathy when engaging in cyber-conflict with Estonia and Georgia, and responded with the denials that typically accompany cyber-attacks.

## **II. The Indications & Warnings of Integrated Cyber-Warfare**

Perhaps the most impressive aspect of Russia's cyber-offensive on Georgia was how it prosecuted its air-campaign in tandem with its cyber-campaign. As the US Cyber Consequences Unit noted in their report on the Russo-Georgian war, the cyber-campaigns primary objective was to support a Russian invasion, and "...the cyber-attacks fit neatly into the invasion plan."<sup>49</sup> As previously noted, the cyber-targets were woven in with the ground and air attacks in such a way that targets were not hit needlessly. If a Georgian capability was not available to be attacked via cyber, due perhaps to the Georgian's lack of technological dependence and minimal CPS, then Russia would hit it physically. Conversely, if a target had been effectively neutered via cyber, Russia would not waste physical resources on hitting it physically, as in the example of Georgian news media outlets.<sup>50</sup>

In addition to the situations where targets were divided by capability, cases also existed where a physical strike on a Georgian asset was supported by a subsequent cyber-strike on a virtual one, as in the case of the previously discussed Georgian generator rental website. While seemingly inconsequential to the layman, this example is very demonstrative of the prior coordination involved in this campaign as well as sophisticated Russian tactics. Hitting this website after physical strikes on the Georgian power-grid effectively neutralizes a possible mitigation tactic of the target. Additionally, cyber-targets were kept in the same general locale in South Ossetia where the physical fighting was occurring, another possible Indicator and Warning for those that were paying attention.<sup>51</sup>

For those that are unfamiliar, a common term in the Intelligence community is Indications and Warnings, or I&W. Russia's campaign against Georgia, and in some ways Estonia as well, provided the intelligence experts in those countries with I&W. If an adversary focuses its cyber-attacks on a certain area, that may provide useful I&W for an intelligence analyst. This might indicate that attacks in the physical domain are going to also be focused on that region, which in turn can be useful in other ways as well. As stated previously, analysts can look at targets that they are expecting to be struck by cyber and have not been. This might indicate an area that would have to be focused on in the physical domain. While tougher in cases like Estonia where there was not a lot of warning, I&W can still be utilized. Something as simple as looking at where the attack is being focused can still tell an analyst something, whether the enemy is using misdirection or not. Without listing all the possibilities, it should be clear that by understanding how a cyber-war is prosecuted, one can take advantage of this knowledge and put it to use in defending oneself in the future.

### **III. Tools and Tactics**

There are countless cyber-tools a state can bring to bear against an adversary, and these can be used in various ways to deny an adversary access to their own systems, disrupt their communications, degrade their capabilities, and even destroy systems altogether. Examples of this range from the Stuxnet virus inserted into Iranian nuclear CPS', allegedly by US and Israeli hackers, to Chinese military hackers establishing a "digital beachhead" in US military computers through the use of an "infected" USB.<sup>52,53</sup> From Russia, the drug of choice appears to primarily be DDoS attacks. This is both good and bad news for those that would anticipate the possibility of having to contend with Russian hackers.

The good news is that both the Estonian and Georgian cases point to DDoS as being the preferred Russian cyber-tactic. To be sure, there were other tactics, such as posting propaganda on Estonian and Georgian government sites, but DDoS seems to be the “tip of the spear.” The bad news is that DDoS, while typically brutish and unsophisticated, can be a fairly effective tactic. In the spectrum of offensive cyber effects, the “five D’s” are deny, degrade, disrupt, destroy, and deceive.<sup>54</sup> DDoS could fall under the various categories of deny, degrade, or disrupt, depending on how effective the attack is. The effectiveness of the attack depends greatly on how large the DDoS capability is.

Part of this research was involved in ascertaining the Russian DDoS capability in terms of size, or Gbps (Gigabytes per second). This information could be applied to the recommendations of this report in order to better prepare the USAF for DDoS mitigation. The methodology involved comparing the size of the Russian DDoS attacks on Estonia and Georgia to the largest known attacks at that time to see if and how much the capabilities of Russia exceeded the attacks of non-state actors. While this research was partially conducted, it became clear from the outset that nothing seminal would be learned from conducting this comparison because of the smaller size of the DDoS attacks. For instance, two years prior to the DDoS attacks on Estonia, the largest attack observed was over 8 Gbps, very large for the time. In 2007, just prior to the Estonian attacks, the largest DDoS attack observed was 24 Gbps.<sup>55</sup> However, the attacks on both Estonia and Georgia were unimpressive in size, sitting just around 1 Gbps.

Is the conclusion then that Russia has such poor capabilities in the cyber-realm that it was unable to muster even 1/24<sup>th</sup> the DDoS attack size that most technically savvy teenagers were capable of at the time? While this information was useless in ascertaining the DDoS capabilities of Russia, it does speak to Russian tactics. 1 Gbps was indeed a comparatively small DDoS

attack at the time. However, it was all that was needed to overcome the bandwidth of the smaller networks used by Estonia, and subsequently Georgia. Not only was discretion utilized in the form of which sites to attack and which to leave alone, Russia appeared to be using only what was needed in order to take the network down. If this was the case, then a larger attack would do nothing but betray a capability better left hidden.

Additionally, while the Russian DDoS attacks were small, they were sophisticated. Most DDoS attacks can be kept up for hours or even a day if the hackers are persistent, but eventually the target is able to patch the system or write filters that will keep the offending requests out. The DDoS attacks on Estonia were sustained for weeks.<sup>56</sup> This takes an active and persistent hacker working around the filters placed by the target in order to block the attack. According to the US-CCU Report on the Georgian Cyber Campaign, the DDoS attacks on Georgia took years of planning to carry out; another indication that Russian cyber-tactics are anything but sophomoric in nature.<sup>57</sup>

In the case study of Russia v. Estonia, Russia effectively pressed the mute button on their capability to communicate through the use of DDoS. In Estonia's case, this was more nuisance than dire problem. Despite losing substantial money from banking and news revenue, the country was not being invaded. Regardless, it is chilling to see what a fairly simple DDoS campaign can do. In the case of Georgia however, we see that not only were Georgian communications affected, they were also rendered blind from a network standpoint by a combination of airstrikes and cyber-attacks on their C2 structures. While this may seem debilitating to readers from technologically advanced states, looking at how Georgia was affected, or rather unaffected, is significant in comparison to Estonia.

There is no doubt that Estonian and Georgian networks were heavily affected where targeted. Estonia was certainly more affected by the attacks due to their technological dependence, but more striking is the lack of adverse effects to the Georgian military. Out of the various networks and websites affected by the cyber-attacks on Georgia, the Georgian military came away all but unscathed. While Georgia has come a long way since 2007 in terms of their information and communication technologies (ICTs), they still have a long way to go.<sup>58</sup> While the World Economic Forum does not assess military dependence on ICTs, if Georgia's government participation in ICTs can be used as a comparable yardstick, Georgia is ranked 60<sup>th</sup> in the world, as opposed to Estonia's ranking of 22<sup>nd</sup> overall.<sup>59</sup> Yet this lack of ICTs had the silver-lining of shielding the potential effects of the cyber-offensive on the Georgian military. Had there been a larger dependence, their effectiveness in the field could have been impacted in a more adverse manner. The oft-cited example of Stuxnet applies here. Had the Iranian centrifuges not been part of a CPS, then their physical systems would not have been able to be targeted in that way. This shines a light on the positives and negatives of cyber-dependence.

In addition to utilizing DDoS to try and blind and gag their targets, Russia appeared to use DDoS as a distraction in some cases by causing a large outage in one sector while conducting cyber-infiltration efforts in another, similar to how DDoS was used during the Sony data breach in 2011.<sup>60</sup> The idea behind this tactic is that while the defensive efforts are being focused on filtering out the incoming data flow from the DDoS attacks, other hackers are moving in to either import harmful virus' and spyware, or export protected data from the target systems. Depending on the nature of the stolen information, it could take the form of economic espionage or even assist with future attacks by giving the hackers a blueprint of the target network's infrastructure and other CPS' that it may be connected to. One final point here; Georgia's most

popular hacking website, [www.hacking.ge](http://www.hacking.ge), was targeted by Russian hackers prior to the main conflict.<sup>61</sup> Part of degrading the opponent is ensuring that it cannot foil an attack or respond in kind.





## **CHAPTER SIX – CONCLUSIONS AND RECOMMENDATIONS**

The following three sets of conclusions and recommendations are based solely on the research and analysis conducted for this report. This should not be viewed as all-inclusive as it relates to anticipating the tactics of an enemy cyber-tactician. Even after exhaustive research on the subject, there are many unknowns in this relatively new domain of war. Nevertheless, following the recommendations of this report will undoubtedly put the USAF, and any other organizations that wish to protect their systems from enemy exploitation during warfare, in better stead for future cyber-conflicts.

### **Conclusion I: Cyber-Attacks Inside and Outside of War**

Imagine if instead of hitting Iran's nuclear centrifuge facility with a computer virus, Israel (one of the alleged perpetrators of the Stuxnet virus) instead conducted an airstrike on the Natanz nuclear facility. Would the Iranian reaction have been the same? One of these actions is a clear violation of sovereign territory and an act of war. The fact that these two actions are deemed different is a troubling reality that the USAF needs to be prepared for. In no other domain would a blatant attack that debilitates a country's ability to communicate, carry out government processes, or conduct business and commerce be allowed to stand without consequence. The actions of Russia in using cyber as a weapon in Estonia and Georgia, and more importantly the world's response to it, point to Conclusion I of this report: the USAF should expect symmetric adversaries to take advantage of the world's apparent apathy about cyber-attacks by carrying out physically detrimental cyber-attacks inside and outside a state of open-conflict.

## **Recommendation I: Protocol for Proportional Cyber-Response**

According to a report conducted by the Center for Strategic and International Studies (CSIS), cyber-attacks, cyber-espionage, and the online pilfering of intellectual property (IP) from the US government and corporate America constitutes an average loss of over \$100 billion dollars annually.<sup>62</sup> That is a serious number that has only risen in recent years, and more serious is that the US alleges that the state of China is responsible for the lion's share of those losses.<sup>63</sup> Taking into consideration the fact that the CSIS report was funded by McAfee, a leading virus-detection software company, the reader might want to assume that number was rounded up, but the point is this: even rounding down a few billion dollars still points to the fact that the status quo of allowing state or state-sponsored cyber-attacks to continue without a response can be extremely harmful and will only serve to embolden an adversary.<sup>64</sup> This leads to Recommendation I: the 24<sup>th</sup> AF, in conjunction with the cyber-divisions of sister services, needs to establish a proportional response protocol for state or state-sponsored cyber-attacks. Owing to the potential seriousness of actions taken under this protocol, a cyber-response in kind would require approval by the Secretary of Defense (SECDEF) or National Security Council (NSC) at the very least.

In 2011, the Pentagon concluded that a cyber-attack can be considered an act of war, but this is not necessarily accepted at the international level.<sup>65</sup> One must note from analysis of this subject that in the case of Russia v. Georgia, though Russia attacked Georgia via cyber weeks prior, Georgia is viewed as the initiator of the conflict since they acted first in the physical realm. In light of this, Recommendation I needs to be an open, transparent, and internationally communicated protocol. The USAF and sister services would be required to openly publish "electronic evidence" that the attack occurred, that actual damage was incurred, and the indicated

author of the attack. It is highly recommended that the US uses the Diplomatic and Economic “Elements of Power” at its disposal to push for other countries to follow suit with similar policies in order for this protocol to become internationally recognized as a norm.

Since these attacks could, as in the case of Estonia and Georgia, be blamed on rogue citizens of the offending country, consideration needs to be taken on how the USAF’s cyber-response will be prosecuted. For instance, in the expected case that the offending country attempts to shift blame onto individual citizens, the country will still be held responsible for failing to prevent their citizen’s actions and be given the option to pay reparations prior to a proportional cyber-response. This recommendation should be considered a long-term objective since the international community is a slow moving body. International law is not necessarily based on hard and fast rules, but rather commonly accepted norms. In pursuing Recommendation I, the USAF can begin to shift the international conversation towards an environment where cyber-apathy is no longer the status quo.

## **Conclusion II: Integrated Domains of Warfare**

Through careful analysis of the Georgian case study, it was shown that the Russian’s are proficient at integrating the disparate domains of warfare. Examples demonstrated how a Russian airstrike was supported by a cyber-attack of secondary or tertiary targets. Additionally, air and ground attacks were withheld from targets that had been neutered by a DDoS attack, and vice-versa. Thus, Conclusion II is that during an open and declared conflict with an enemy state, the USAF should expect a technically symmetric adversary to employ a sophisticated campaign of cyber-warfare that is actively integrated with the air, space, land, and sea domains of warfare.

## **Recommendation II: Cyber-ISR Assessment Teams**

Cyberspace is an extremely prolific source for predictive Intelligence, Surveillance, and Reconnaissance (ISR) sensing-activities. As was noted in the case of Russia v. Georgia, hacker activities appeared to be anything but random.<sup>66</sup> Furthermore, according to the Director of the National Security Agency (NSA), roughly 95% of cyberspace operations are dedicated to ISR, so cyber is by no means an ignored sector of ISR.<sup>67</sup> In response to the conclusion that a symmetric enemy will integrate its cyber-campaign with other warfare domains, Recommendation II is that the USAF needs to take advantage of the inherent I&W that accompanies cyber-activities during an integrated enemy campaign.

The first half of this equation is utilizing the Cyberspace Professional Development Program, or CPDP. The CPDP is the governing program for Air Force cyberspace force development.<sup>68</sup> By placing an emphasis on incorporating real-time assessment skills into the professional development of its ISR analysts through the CPDP, the USAF can turn an adversary's strength into a weakness by exploiting the ISR indicators inherent in their cyber-campaign. Further, it is recommended that the USAF places an emphasis on Attack Sensing and Warning (AS&W) and I&W as it pertains to conducting ISR on integrated cyber-warfare activities by incorporating this training into the Intelligence Officer Career Field Education and Training Plan.

The recommended course would take the form of a cyber-ISR training module. This module would be focused on how to go about creating cyber-ISR teams, as part of Crisis Action Planning (CAP), by marrying the ISR AFSCs that have been focused on cyber AS&W and I&W training through the CPDP, with those AFSCs in the cyber community that are familiar with rapidly gathering the data needed to make these assessments – namely, but not limited to, 1B4Xs

(Network Warfare Operator). These teams would make real-time threat assessments on possible friendly centers of gravity (CoG) based on where cyber is and is not being utilized by the adversary.

If these teams do their homework (quickly), it may be possible to predict where strikes will occur based on what the adversary is and is not attacking via-cyber, and then funnel that information quickly up the C2 chain to the decision makers. Best of all, these rapid ISR communication chains already exist in the form of "...warning communications channels and procedures [giving] the Department of Defense the ability to sense changes in DoD information networks...including the detection, correlation, identification, and characterization of a large spectrum of intentional unauthorized activity, including an intrusion or attack."<sup>69</sup>

Bodeau and Groubart point out that at a heightened level of training, "...AS&W cyber-monitoring can make adversary activities visible to defenders" which, if exploited, can help counter a sophisticated, integrated enemy cyber-campaign.<sup>70</sup>

### **Conclusion III: Taking Advantage of Tech-Dependence**

Both case studies featured a variety of Russian cyber-attacks, including network infiltration, malware insertion, and propaganda by way of website defacement, but the tactic *du jour* appeared to be the use of DDoS. Since DDoS attacks are alternately capable of denying, degrading, disrupting, and deceiving the target systems and users, it appears to be the most prolific and tactically diverse of Russian tactics used. Based on observations of Russian actions during the Estonian and Georgian campaigns, Conclusion III is that the USAF should expect a technically symmetric adversary to utilize a variety of cyber-attacks, but its primary tactic will be to exploit the US military's heavy dependence on technology by employment of the DDoS

attack. Further, it is concluded that the adversary will use the DDoS attack to blind the US military and deny the communication capabilities of its C2 facilities, networks, and personnel.

### **Recommendation III: Evolving DDoS Mitigation and Cyber-ATSO Training**

The type of attack most likely to be utilized by an adversary in or prior to the outset of a conflict will be the DDoS attack. This attack will be an effort to take advantage of a technologically dependent military force. As should be fairly obvious, the lesson here is not to unplug. It can be fairly assumed that the benefits of having a high ICT index in today's globalized internet infrastructure far outweigh the danger of having potentially exploitable networks. That is not to say that caution should not be exercised.

Unfortunately, due to the lack of observable examples of substantial Russian DDoS activity (in terms of Gbps) during the case studies analyzed, the upper limitations of Russian DDoS capabilities is still an unknown vis-à-vis this research. However, it must be understood that using the size of an adversary's DDoS attack as a measurement of capability is going to only capture a moment in time. DDoS capabilities are constantly evolving as technology advances. For instance, earlier in the report it was pointed out that a 24 Gbps DDoS attack in 2007 was an upper-tier capability. However, in 2014 a 400 Gbps DDoS attack was observed.<sup>71</sup> Therefore, if one is to make an assumption on the DDoS capabilities of a technologically prolific adversary, it would be safest to assume that their capabilities at least meet or generally exceed the largest currently observed DDoS attack on record.

For Conclusion III, a two-part recommendation is needed. Part one of Recommendation III is that the USAF needs to either field or contract a "Cloud" style DDoS-mitigation system with the capability to handle at least three times the largest known DDoS attack currently on

record. As a reminder to the reader, these “observed” DDoS attacks that occur daily throughout the world are for the most part coming from individual or collaborative efforts of non-state actors. As such, it is operationally conservative to assume that should a large state actor bring its substantial resources to bear on creating a DDoS botnet, it will assuredly be on par, or more likely, even larger than what is currently being observed on global networks.

The good news is that the USAF is currently fulfilling the first part of Recommendation III. As this report cannot go beyond the unclassified level, a specific look at the USAF’s DDoS mitigation capabilities will not be discussed here. However, it must be further pointed out that whatever method the USAF employs to mitigate DDoS attacks against the AFIN, the delta will constantly change on what the accepted level of mitigation capability is. Therefore, this capability must be in constant measurement against the evolving real-world capabilities of the hacker community to stay ahead of the curve.

While the USAF should make every effort to deny the enemy’s capability to carry out a successful DDoS attack on the AFIN, it would be folly to assume an adversary could not successfully deny a capability, or at least degrade it temporarily, through the use of DDoS. Based in part on this as well as the conclusion that the most likely enemy course of action (ECOA) regarding the cyber-tactic of DDoS will be to degrade the USAFs operational picture and ability to communicate with its assets, the second part of Recommendation III is that the USAF salt its heavy dependence on technology in warfare by developing exercises designed to test the capabilities of its Airmen to operate in a technologically degraded environment. Furthermore, it is recommended that capabilities be developed or reintroduced into common practice that may have previously been regarded as “legacy” or obsolete.

Exercises should give heavy consideration to prosecuting wartime C2 via degraded

technological means. In execution, these exercises can be conducted in a similar manner to the already effective Ability to Survive and Operate (ATSO) exercises. Instead of surviving a Nuclear, Biological, or Chemical attack however, Airmen would come under an effective cyber-attack. The unit or operations center would then be asked to continue normal operations under degraded conditions. In this way, the USAFs weaknesses to this type of attack would be exposed, and could then be subsequently shored up in an appropriate manner.

### **Recommendations for Future Research:**

This report discussed several “research considerations” that the reader was asked to keep in mind when considering the conclusions and recommendations of this report. When looking to expand upon these conclusions, future researchers can easily find ways to improve upon them by taking note of where this research was limited. If this research was limited in how many conflicts it was able to draw upon for research samples, then simply waiting for new conflicts with integrated cyber-campaigns will undoubtedly lead to either bolstering the conclusions of this report or even being able to discount faulty conclusions made. China has not been shy with its use of the cyber-domain and will undoubtedly be a source for robust research in this area.

Future research is desperately needed in the realm of cyber-kinetics, or the capability of cyber-attacks to go beyond the cyber-domain. As this paper previously alluded to, the apathy on this topic is born of an ignorance of cyber’s ultimate potential. It is only a matter of time until cyber is used in a way that leads to significant damage and possibly loss of life. If future research on this subject can be persuasive enough to sway public opinion on this matter than significant dangers would ideally be avoided. For more information on the potential of cyber-kinetics, readers would do well to read Applegate’s report, *The Dawn of Cyber*.



## Report Summary

The world is continually shrinking in terms of space and resources, a situation that will inevitably lead to conflict. The overall objective of this report was to better prepare the warfighter for an eventual conflict involving integrated cyber-warfare that is all but inevitable. To achieve this end, the research question asked how the USAF, instead of being reactionary, could stay ahead of adversaries by learning from the conflicts of others. The methodology involved analyzing the case studies of Russia v. Estonia and Russia v. Georgia, two conflicts notable due to Russia's use of cyber. Following a discussion of the limitations on this research, primarily involving the relative infancy of this type of warfare, the report engaged in an in-depth analysis of several cyber-tactics utilized by Russian hackers.

The research and analysis of the two case studies produced three overall conclusions vis-à-vis cyber-tactics: a technically symmetric opponent will most likely be willing to strike via cyber regardless of whether a state of open conflict has been acknowledged, cyber-warfare will be effectively integrated with the air, land, sea, and space domains, and lastly, an adversary will look to capitalize upon the USAFs heavy dependence on technology and connectivity to achieve their ends. In light of these conclusions, it was recommended that the USAF take three achievable long and short term actions to protect, defend, and ultimately capitalize on these possible enemy actions.

The first recommendation involved creating an environment where states and state-actors are taken to task in the physical realm for actions they have taken in the cyber domain. Secondly, it was recommended that the USAF incorporate cyber-assessment teams into CAP through enhanced training programs, and by integrating ISR with cyber functions to take advantage of how these disparate career fields complement each other. The final

recommendation of this report was that the USAF needs to employ DDoS mitigation capabilities that are constantly being compared and updated in response to real-world DDoS proliferation and evolution. The second half of the equation for the USAF in protecting itself against the threat of DDoS attacks is by slowly weaning itself off of sole-dependence on technology to prosecute the mission. It was recommended that this be accomplished through the use of exercises focused on working through mission challenges while weathering degraded C2 functions.

This report closed with a short discussion on how future researchers can utilize the conclusions of this research to encourage the discussion of the USAF's vulnerabilities at the highest echelons of the service. It is sincerely hoped that the conclusions and recommendations of this report are able to be utilized, or at the very least, serve to educate the warfighter and encourage more discovery on the important topic of cyber-warfare. This area of study will undoubtedly see much more attention as technology continues to be depended on to win the fight.

## ENDNOTES

- 
- <sup>1</sup> Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *JSS* 4, no. 2 (Journal of Strategic Studies, Summer 2011, 49-60): 51.
- <sup>2</sup> David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal* (Small Wars Foundation, 6 January, 2011): 1-10.
- <sup>3</sup> Mike Fitzgerald, "Scott Air Force Base Poised for Military Cybersecurity Boom," *Belleville News Democrat*, 2014, <http://www.bnd.com/2014/07/12/3299436/scott-air-force-base-poised-for.html>.
- <sup>4</sup> "DDoS Attack Timeline: The History and Changing Nature of DDoS Attacks," *Defense.net*, 2014, <http://www.defense.net/ddos-attack-timeline.html>.
- <sup>5</sup> Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *WIRED*, 21 August 2007.
- <sup>6</sup> Ellen Nakashima, "Hacker Group Briefly Takes down CIA Web Site," *The Washington Post*, 16 June 2011. <http://www.highbeam.com/doc/1P2-28930583.html?>
- <sup>7</sup> Fitzgerald, "Scott Air Force Base Poised for Military Cybersecurity Boom."
- <sup>8</sup> Air Force Instruction (AFI) 33-115, *Communications and Information: Air Force Information Technology (IT) Service Management*, Sep 2014, 3.
- <sup>9</sup> Igal Zeifman, "Q3 2015 Global DDoS Threat Landscape Report," November 2015, <https://www.incapsula.com/blog/ddos-threat-landscape-report-q3-2015.html>.
- <sup>10</sup> Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," 50.
- <sup>11</sup> "NATO Sees Recent Cyber Attacks on Estonia as Security Issue," *DW*, 26 May 2007, <http://www.dw.com/en/nato-sees-recent-cyber-attacks-on-estonia-as-security-issue/a-2558579>.
- <sup>12</sup> Sources differ on day of actual removal, from April 27-30; consensus appears to be April 27 for the removal of the Bronze Soldier. Differing sources: *Ibid*, and Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses."
- <sup>13</sup> Steven Myers, "Russia Rebukes Estonia for Moving Soviet Statue," *The New York Times*, 26 April 2007, <http://www.nytimes.com/2007/04/27/world/europe/27cnd-estonia.html?pagewanted=print>.
- <sup>14</sup> Davis, "Hackers Take Down the Most Wired Country in Europe."
- <sup>15</sup> Kertu Ruus, "Cyber War I: Estonia Attacked from Russia," *European Affairs* 9, no. 1-2 (Winter/Spring 2008), <http://www.europeaninstitute.org/index.php/42-european-affairs/winterspring-2008/67-cyber-war-i-estonia-attacked-from-russia>.
- <sup>16</sup> Davis, "Hackers Take Down the Most Wired Country in Europe."
- <sup>17</sup> Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," 52.
- <sup>18</sup> Kertu, "Cyber War I: Estonia Attacked from Russia."
- <sup>19</sup> "The Cyber Raiders Hitting Estonia," *BBC News*, 17 May 2007, <http://news.bbc.co.uk/2/hi/europe/6665195.stm>.
- <sup>20</sup> Andreas Schmidt, "The Estonian Cyberattacks," in *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, ed. Jason Healey. Cyber Conflict Studies Association, (2013). 1-28.
- <sup>21</sup> *Ibid*.
- <sup>22</sup> Davis, "Hackers Take Down the Most Wired Country in Europe."
- <sup>23</sup> Schmidt, "The Estonian Cyberattacks," 1-28.
- <sup>24</sup> *Ibid*.
- <sup>25</sup> Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," 51-52.
- <sup>26</sup> *Georgia: Avoiding War in South Ossetia*, ICG Report 159, (Brussels, Belgium: International Crisis Group, 26 November 2004), <http://www.crisisgroup.org/en/regions/europe/south-caucasus/georgia/159-georgia-avoiding-war-in-south-ossetia.aspx.7-8>.
- <sup>27</sup> *Ibid*, 1-13.
- <sup>28</sup> "Russia-Georgia Conflict: Why Both Sides Have Valid Points," *The Christian Science Monitor*. 19 August 2008, <http://www.csmonitor.com/World/Europe/2008/0819/p12s01-woeu.html>.
- <sup>29</sup> *Ibid*.
- <sup>30</sup> Julie A. George, *The Politics of Ethnic Separatism in Russia and Georgia*, (New York, NY [or N.Y.]: Palgrave Macmillan, 2009), 181.
- <sup>31</sup> *Ibid*.
- <sup>32</sup> Eneken Tikk, et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, Cooperative Cyber

---

Defense Center of Excellence (Tallinn, Estonia, November 2008), <http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf>. 4.

<sup>33</sup> Hollis, "Cyberwar Case Study: Georgia 2008," 1-10.

<sup>34</sup> John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, 12 August 2008, [http://www.nytimes.com/2008/08/13/technology/13cyber.html?\\_r=1](http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1).

<sup>35</sup> Ibid.

<sup>36</sup> Gregg Keizer, "Russian Hacker 'Militia' Mobilizes to Attack Georgia," *Network World*, 13 August 2008, <http://www.networkworld.com/news/2008/081208-russian-hacker-militia-mobilizes-to.html>.

<sup>37</sup> John Bumgarner, *The US-CCU Report on the Georgian Cyber Campaign*, US Cyber Consequences Unit (Redwood Shores, CA [or C.A.], August 2008), <https://www.incapsula.com/blog/ddos-threat-landscape-report-q3-2015.html>, 6.

<sup>38</sup> Ibid.

<sup>39</sup> Ibid.

<sup>40</sup> Tikk et al., "Cyber Attacks Against Georgia: Legal Lessons Identified," 5.

<sup>41</sup> Bumgarner, "The US-CCU Report on the Georgian Cyber Campaign," 6.

<sup>42</sup> Tikk, et al., "Cyber Attacks Against Georgia: Legal Lessons Identified," 32.

<sup>43</sup> Schmidt, "The Estonian Cyberattacks," 1-28.

<sup>44</sup> Ibid.

<sup>45</sup> Tikk et al., "Cyber Attacks Against Georgia: Legal Lessons Identified," 4-5.

<sup>46</sup> Rehman Scheherazade, "Estonia's Lessons in Cyberwarfare," *US News & World Report*, January 2014, <http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare>.

<sup>47</sup> Scott D. Applegate, *The Dawn of Kinetic Cyber*, Center for Secure Information Systems (Fairfax, VA [or V.A.] 2013), 2.

<sup>48</sup> Ibid.

<sup>49</sup> Bumgarner, "The US-CCU Report on the Georgian Cyber Campaign," 6.

<sup>50</sup> Ibid.

<sup>51</sup> Hollis, "Cyberwar Case Study: Georgia 2008," 6.

<sup>52</sup> James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War Online," IISS (London, England. International Institute for Strategic Studies, 28 January 2011), 33.

<sup>53</sup> William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September/October 2010.

<sup>54</sup> Air Force, "Air Force Cyber Command Strategic Vision," Air Force Cyber Command (Barksdale AFB, LA [or L.A.], February 2008), 13.

<sup>55</sup> "DDoS Attack Timeline: The History and Changing Nature of DDoS Attacks."

<sup>56</sup> Schmidt, "The Estonian Cyberattacks," 11.

<sup>57</sup> Bumgarner, "The US-CCU Report on the Georgian Cyber Campaign," 6.

<sup>58</sup> "Network Readiness Index," World Economic Forum, 2015, <http://reports.weforum.org/global-information-technology-report-2015/network-readiness-index/>.

<sup>59</sup> Ibid.

<sup>60</sup> "DDoS Attack Timeline: The History and Changing Nature of DDoS Attacks."

<sup>61</sup> Tikk et al., "Cyber Attacks Against Georgia: Legal Lessons Identified," 9.

<sup>62</sup> Ellen Nakashima and Andrea Peterson, "Report: Cybercrime and espionage costs \$445 billion annually," *The Washington Post*, 9 June 2014, [https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a\\_story.html](https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html).

<sup>63</sup> Ibid.

<sup>64</sup> Ibid.

<sup>65</sup> Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War, Pentagon Sets Stage for U.S. to Respond to Computer Sabotage With Military Force," *The Wall Street Journal*, 31 May 2011, <http://www.wsj.com/articles/SB10001424052702304563104576355623135782718>.

<sup>66</sup> Deborah Bodeau and Richard Graubart, *Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment*, The MITRE Corporation, Bedford, MA [or M.A.], November 2013, 18.

<sup>67</sup> Air Force, "Intelligence Officer Career Field Education and Training Plan," Department of the Air Force, (Washington, DC [or D.C.], 13 February 2013), 17.

---

<sup>68</sup> Ibid.

<sup>69</sup> CJCSM 6510.01B, “Cyber Incident Handling Program,” Joint Chiefs of Staff (Washington DC [or D.C.]: 10 July 2012), A-7.

<sup>70</sup> Bodeau and Graubart, *Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment*, The MITRE Corporation (Bedford, MA [or M.A.], November 2013), 35.

<sup>71</sup> “DDoS Attack Timeline: The History and Changing Nature of DDoS Attacks.”



## BIBLIOGRAPHY

- Air Force. Air Force Cyber Command Strategic Vision. Air Force Cyber Command, Barksdale AFB, LA [or L.A.]. February 2008.
- Air Force Instruction (AFI) 33-115, Communications and Information: Air Force Information Technology (IT) Service Management. September 2014.
- Air Force. "Intelligence Officer Career Field Education and Training Plan." Department of the Air Force. (Washington, DC [or D.C]: 13 February 2013).
- Applegate Scott D. *The Dawn of Kinetic Cyber*. Center for Secure Information Systems. Fairfax, VA [or V.A.]. 2013.
- Bodeau, Deborah and Richard Graubart. *Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment*. The MITRE Corporation. Bedford, MA [or M.A.]. November 2013.
- Bumgarner, John. *The US-CCU Report on the Georgian Cyber Campaign*. US Cyber Consequences Unit, August 2008. Shores, CA [or C.A.], November 2015. <https://www.incapsula.com/blog/ddos-threat-landscape-report-q3-2015.html>
- CJCSM 6510.01B. "Cyber Incident Handling Program." Joint Chiefs of Staff (Washington DC [or D.C.]: 10 July 2012).
- Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe." *WIRED*. 21 August 2007. <http://www.wired.com/2007/08/ff-estonia/>
- "DDoS Attack Timeline: The History and Changing Nature of DDoS Attacks." Defense.net. 2014.
- Farwell, James P. and Rafal Rohozinski. "Stuxnet and the Future of Cyber War Online." IISS. London, England. International Institute for Strategic Studies, 28 January 2011
- Fitzgerald, Mike. "Scott Air Force Base Poised for Military Cybersecurity Boom." *Belleville News-Democrat*, 2014. <http://www.bnd.com/2014/07/12/3299436/scott-air-force-base-poised-for.html>
- George, Julie A. *The Politics of Ethnic Separatism in Russia and Georgia*. New York, NY [or N.Y.]: Palgrave Macmillan, 2009.
- Georgia: Avoiding War in South Ossetia*. ICG Report 159. Brussels, Belgium: International Crisis Group, 26 November 2004. <http://www.crisisgroup.org/en/regions/europe/south-caucasus/georgia/159-georgia-avoiding-war-in-south-ossetia.aspx>.

- Gorman, Siobhan and Julian E. Barnes. "Cyber Combat: Act of War, Pentagon Sets Stage for U.S. to Respond to Computer Sabotage with Military Force," *The Wall Street Journal*, 31 May 2011, <http://www.wsj.com/articles/SB10001424052702304563104576355623135782718>
- Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2, (Summer, 2011): 49-60. <http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss>
- Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*. Small Wars Foundation, (6 January, 2011): 1-10.
- Keizer, Gregg. "Russian Hacker 'Militia' Mobilizes to Attack Georgia." *Computerworld*, 12 August 2008. <http://www.networkworld.com/news/2008/081208-russian-hacker-militia-mobilizes-to.html>
- Lynn, William J. III "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs*. September/October 2010.
- Markoff, John. "Before the Gunfire, Cyberattacks." *New York Times*, 12 August 2008. [http://www.nytimes.com/2008/08/13/technology/13cyber.html?\\_r=1](http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1)
- Myers, Steven. "Russia Rebukes Estonia for Moving Soviet Statue." *The New York Times*. 26 April 2007. <http://www.nytimes.com/2007/04/27/world/europe/27cndestonia.html?pagewanted=print>.
- Nakashima, Ellen. "Hacker Group Briefly Takes down CIA Web Site." *The Washington Post*, 16 June 2011. <http://www.highbeam.com/doc/1P2-28930583.html?>
- Nakashima, Ellen and Andrea Peterson. "Report: Cybercrime and espionage costs \$445 billion annually." *The Washington Post*. 9 June 2014. [https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a\\_story.html](https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html)
- "NATO Sees Recent Cyber Attacks on Estonia as Security Issue." *DW*. 26 May 2007. <http://www.dw.com/en/nato-sees-recent-cyber-attacks-on-estonia-as-security-issue/a-2558579>.
- "Network Readiness Index." World Economic Forum, 2015. <http://reports.weforum.org/global-information-technology-report-2015/network-readiness-index/>
- "Russia-Georgia Conflict: Why Both Sides Have Valid Points." *The Christian Science Monitor*. 19 August 2008. <http://www.csmonitor.com/World/Europe/2008/0819/p12s01-woeu.html>



- Ruus, Kertu. "Cyber War I: Estonia Attacked from Russia." *European Affairs* 9, no. 1-2 (Winter/Spring 2008). <http://www.europeaninstitute.org/index.php/42-european-affairs/winterspring-2008/67-cyber-war-i-estonia-attacked-from-russia>.
- Scheherazade, Rehman. "Estonia's Lessons in Cyberwarfare." *US News & World Report*. January 2014. <http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare>
- Schmidt, Andreas. "The Estonian Cyberattacks." In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Edited by Jason Healey. Cyber Conflict Studies Association, 2013.
- "The Cyber Raiders Hitting Estonia." *BBC News*. 17 May 2007. <http://news.bbc.co.uk/2/hi/europe/6665195.stm>.
- Tikk, Eneken et al. *Cyber Attacks Against Georgia: Legal Lessons Identified*. Cooperative Cyber Defense Center of Excellence, Tallinn, Estonia, November 2008. <http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf>.
- Zeifman, Igal. Q3 2015 Global DDoS Threat Landscape Report. Imperva Incapsula, Redway Shores, CA [or C.A.], November 2015. <https://www.incapsula.com/blog/ddos-threat-landscape-report-q3-2015.html>

